

Information Security

Introduction to Cryptography

Lecturer: Nguyễn Thị Thanh Vân – FIT - HCMUTE

Contents

- ∞ **History of Encryption**
- ∞ **Substitution Techniques:** Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Polyalphabetic Ciphers
- ∞ **Transposition Techniques: Rail Fence**
- ∞ **Symmetric and asymmetric encryption**
- ∞ **Hash**
- ∞ **Digital signatures**

Introduction

- ∞ Cryptography is technique of securing information and communications through use of codes so that only those person for whom the information is intended can understand it and process it.
 - Thus preventing unauthorized access to information.
- ∞ Cryptography
 - The prefix “crypt” means “hidden” and
 - suffix “graphy” means “writing”.

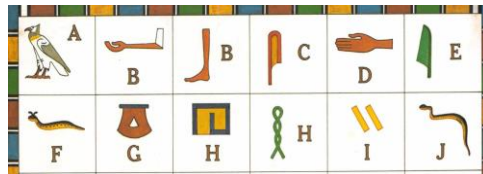
22/08/2024

3

History of Encryption

∞ Classical cryptography

- History of cryptography is over than 3,000 years
- The object of the cryptography is **characters**
- Encryption/Decryption is performed manually or by using mechanical principles
- Applied commonly in military
 - A series of three rotors from an Enigma machine, used by Germany Military during World War II



4

History of Encryption

Modern cryptography (since 1970)

- Beginning with the development of Computer and Information Technology
- Processing by Computer using **bits**
- Applying widely in many fields, especially in electronic transactions



5

Cryptography in Action

- ❖ Some examples of applied cryptography are:
 - ❖ Public key infrastructure (PKI)
 - ❖ Digital certificates
 - ❖ Authentication
 - ❖ E-commerce
 - ❖ RSA
 - ❖ MD-5
 - ❖ Secure Hash Algorithm (SHA)
 - ❖ Secure Sockets Layer (SSL)
 - ❖ Pretty Good Privacy (PGP)
 - ❖ Secure Shell (SSH)

22/08/2024

6

Applications of Cryptography

- ☞ Goal: confidentiality
- ☞ Internet Protocol Security (IPSec):
 - a set of protocols designed (to operate at the Network layer of the OSI) to protect the confidentiality and integrity of data as it flows over a network.
- ☞ Pretty Good Privacy (PGP):
 - Using public key encryption, PGP is one of the most widely recognized cryptosystems in the world.
 - PGP has been used to protect the privacy of e-mail, data
- ☞ Secure Sockets Layer (SSL).
 - was developed by Netscape in the mid-1990s and rapidly became a standard mechanism for exchanging data securely over insecure channels such as the Internet.

22/08/2024

7

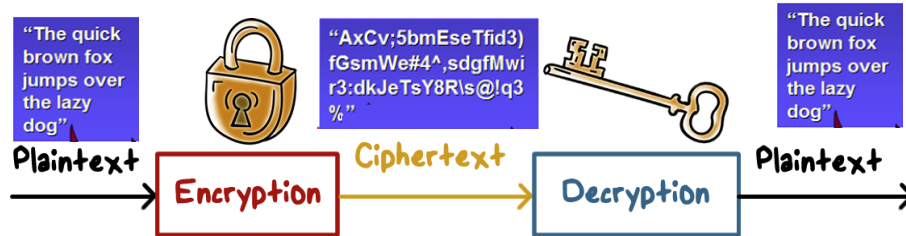
Main terms used in cryptography

- ☞ **Plaintext:** This is the original intelligible message or data that is fed into the algorithm as input.
- ☞ **Encryption algorithm:** The encryption algorithm performs various substitutions and transformations on the plaintext.
- ☞ **Secret key:** The secret key is also input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm.
- ☞ **Ciphertext:** This is the scrambled message produced as output. It depends on the plaintext and the secret key.
- ☞ **Decryption algorithm:** This is essentially the encryption algorithm run in reverse. It takes the ciphertext and the secret key and produces the original plaintext.

22/08/2024

8

So How Does It Work?



- There is a **one-to-one mapping**
- Provides **confidentiality protection**

22/08/2024

9

Mã hóa có đối xứng: key khóa và key giải mã là cùng 1 key Symmetric encryption model

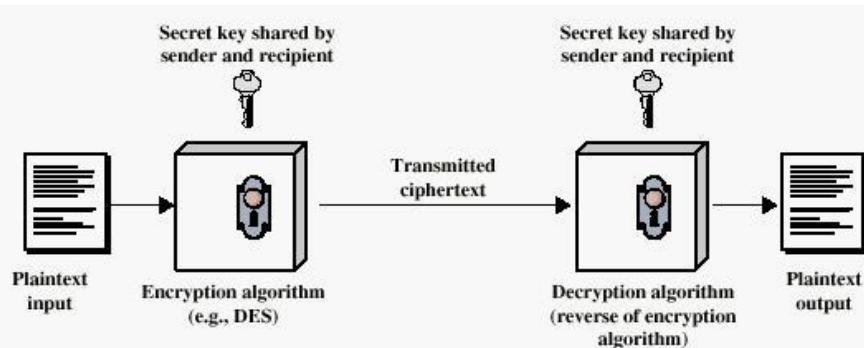


Figure 2.1 Simplified Model of Conventional Encryption

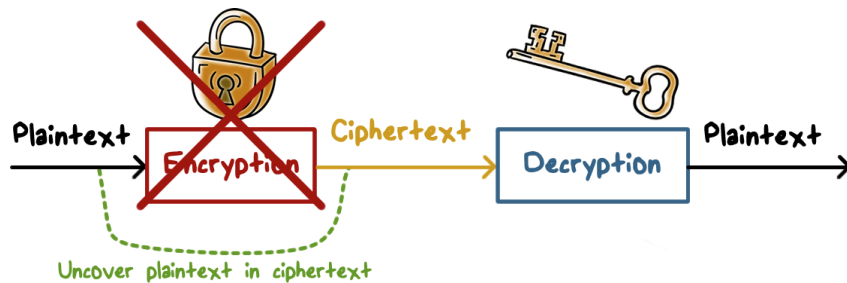
22/08/2024

10

Break a cipher

Break a cipher:

- Uncovering plaintext p from ciphertext c , or, alternatively, discovering the key
- the attacker may try to discover the encryption key so that he can then decrypt all data encrypted using that key.



22/08/2024

11

Attack types on Encryption



•Brute-force attack thử tay mọi trường hợp để tìm KEY

- E.g., try all possible keys

•Cryptanalysis

- Analysis of the algorithm and data characteristics

•Implementation attacks

- E.g., side channel analysis

•Social-engineering attacks

Tấn công dựa vào các mối quan hệ xã hội như birthday, ...

Tấn công triển khai -> Tìm cửa khác, lỗ hổng khác để chui vào thay vì cửa chính

Brute-Force Attack and Cryptanalysis

There are two general approaches to attacking a conventional encryption scheme

Brute-force attack

- Attacker tries every possible key on a piece of ciphertext until an intelligible translation into plaintext is obtained
- On average, half of all possible keys must be tried to achieve success



22/08/2024

Cryptanalysis

- Attack relies on the nature of the algorithm plus some knowledge of the general characteristics of the plaintext
- Attack exploits the characteristics of the algorithm to attempt to deduce a specific plaintext or to deduce the key being used



13

types of cryptanalytic attacks

Type of Attack	Known to Cryptanalyst
Ciphertext Only	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext
Known Plaintext	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext • One or more plaintext–ciphertext pairs formed with the secret key
Chosen Plaintext	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key
Chosen Ciphertext	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key
Chosen Text	<ul style="list-style-type: none"> • Encryption algorithm • Ciphertext • Plaintext message chosen by cryptanalyst, together with its corresponding ciphertext generated with the secret key • Ciphertext chosen by cryptanalyst, together with its corresponding decrypted plaintext generated with the secret key

2

Cipher Strength

☞ A strong algorithm that meets 1 or 2 of the following criteria:

- The cost of breaking the cipher exceeds the value of the encrypted information. (Low value)
- The time required to break the cipher exceeds the useful lifetime of the information. (large time)

☞ Average Time Required for Exhaustive Key Search

Key Size (bits)	Number of Alternative Keys	Time Required at 1 Decryption/ μ s	Time Required at 10^6 Decryptions/ μ s
32	$2^{32} = 4.3 \times 10^9$	$2^{31} \mu s = 35.8$ minutes	2.15 milliseconds
56	$2^{56} = 7.2 \times 10^{16}$	$2^{55} \mu s = 1142$ years	10.01 hours
128	$2^{128} = 3.4 \times 10^{38}$	$2^{127} \mu s = 5.4 \times 10^{24}$ years	5.4×10^{18} years
168	$2^{168} = 3.7 \times 10^{50}$	$2^{167} \mu s = 5.9 \times 10^{36}$ years	5.9×10^{30} years
26 characters (permutation)	$26! = 4 \times 10^{26}$	$2 \times 10^{26} \mu s = 6.4 \times 10^{12}$ years	6.4×10^6 years

Thời gian giải mã phụ thuộc vào độ dài khóa
Chất lượng PC càng tốt thì thời gian giải càng nhanh

Taxonomy of Cryptography

The type of operations used for transforming plaintext to ciphertext

Thay thế
Substitution

Chuyển dịch
Transposition

The number of keys used

MH đối xứng

Symmetric, single-key, secret-key, conventional encryption

MH bất đối xứng

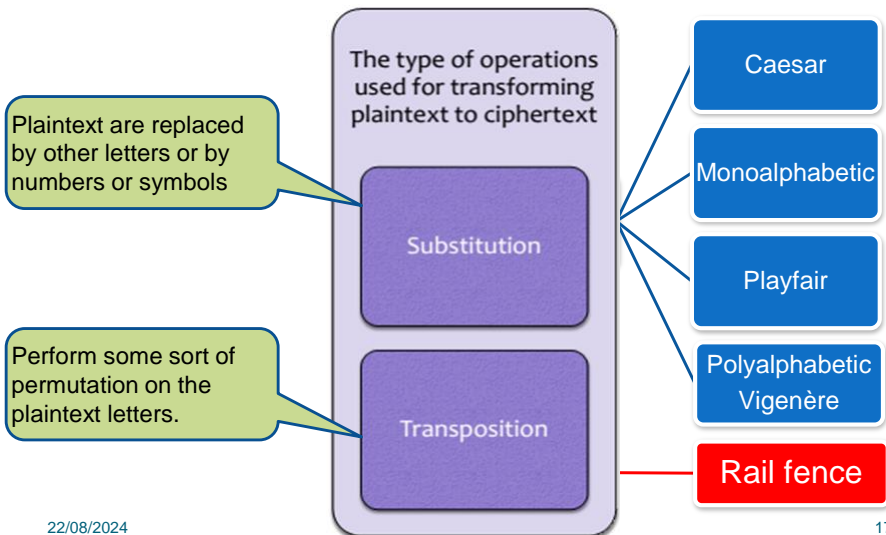
Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed

xử lý theo từng khối
Block cipher

Xử lý theo từng dòng
Stream cipher

Substitution & Transposition



Substitution Technique



Nguyen Thi Thanh Van - Khoa CNTT

22/08/2024

Substitution Technique

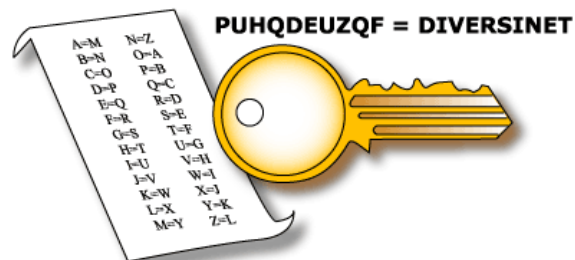
- ☞ Caesar Cipher,
- ☞ Monoalphabetic Ciphers,
- ☞ Playfair Cipher,
- ☞ Polyalphabetic Ciphers

22/08/2024

19

Caesar Cipher: introduction

- ☞ Caesar Cipher: invented by Julius Caesar
 - The earliest known,
 - The simplest,
 - use of a substitution cipher



22/08/2024

20

Caesar Cipher: algorithm

- For each plaintext letter p , substitute the ciphertext letter C , a shift parameter k is used as the key

k (hay key) ở mã hóa Caesar là sự dịch phải k lần trong bảng chữ cái



- Caesar Cipher: $k=3$ Nếu ko cho key thì tự mò $k=1 \rightarrow 25$

- The encryption: $C = E(k, p) = (p + k) \bmod 26$
where k takes on a value in the range 1 to 25.
- The decryption: $p = D(k, C) = (C - k) \bmod 26$
- Other ways: Encryption: $C = (P * K) \bmod 26$
 - For Encryption : $C = (P * K1 * K2) \bmod 26$
 - For Decryption : $P = ((C - K2) / K1) \bmod 26$

24/08/2024

21

Caesar Cipher: Cryptanalysis

- The Caesar cipher can be easily broken by Brute-Force Method:
 - simply try all the 25 possible keys
- 3 important characteristics of cryptanalysis:
 - The encryption and decryption algorithms are known.
 - There are only 25 keys to try.
 - The language of the plaintext is known and easily recognizable (abbreviated or compressed)
- Ex:
 - Encrypt the message $P = \text{hello}$, $k=2 \Rightarrow C = \text{jgnnq}$
 - Decrypt the message $C = \text{pumvythapvu zljbyapf}$ using the Caesar $k=7$. $P=?$
 - Decryption: $C = \text{LQIRUPDWLRQVHFXULWB}$. No key. $P=?$

22/08/2024

22

Cryptanalysis

☞ Brute-Force Cryptanalysis of Caesar Cipher

☞ Ex: Decryption

PHHW PH DIWHU WKH WRJD SDUWB

22/08/2024

KEY	PHHW PH DIWHU WKH WRJD SDUWB
1	oggv og chvgt vjg vqic rctva
2	nffu nf bgufs uif uphb qbsuz
• 3	meet me after the toga party
4	ldds ld zesdq sgd snfz ozgsx
5	kccr kc ydrpc rfc rmev nyprw
6	jbbq jb xcqbo qeb qldx mxoqv
7	iaap ia wbpap pda pkcw lwnpu
8	hzzo hz vaozm ocz ojbv kmot
9	gyyn gy uznyl nby niau julns
10	fxxm fx tymck max mhzt itkmr
11	ewwl ew sxlwj lzw lgys hsjlq
12	dvvk dv rkwvi kyv kfxr grikp
13	cuuj cu qvjuh jxu jewq fqhjo
14	btti bt puitg iwt idvp epgin
15	assh as othsf hvs hcuo dofhm
16	zrrg zr nsgre gur gbtn cnegl
17	yqqf yq mrfqd ftq fasm bmdfk
18	xppe xp lqepc esp ezrl alcej
19	wood wo kpdob dro dyqk zkdbi
20	vnnc vn jocna cqn cxpj yjach
21	ummb um inbmz bpm bwoi xizbg
22	tlla tl hmaly aol avnh whyaf
23	skkz sk glzxx znk zumg vgxe
24	rjyy rj fkyjw ymj ytlf ufwyd
25	qiix qi ejxiv xli xske tevx

Monoalphabetic Ciphers

- ☞ The mapping is done randomly and the difference between the letters is not uniform.
 - a single cipher alphabet is used per message
- ☞ A dramatic increase in the key space can be achieved by allowing an **arbitrary substitution**
- ☞ Permutation
 - A finite set of elements S is an ordered sequence of all the elements of S , with each element appearing exactly once
- ☞ If the “cipher” line can be any permutation of the 26 alphabetic characters, then there are 26! possible keys

24/08/2024

24

Monoalphabetic Ciphers: Cryptanalysis

☞ Easy to break by Brute Force because they reflect the frequency data of the original alphabet:

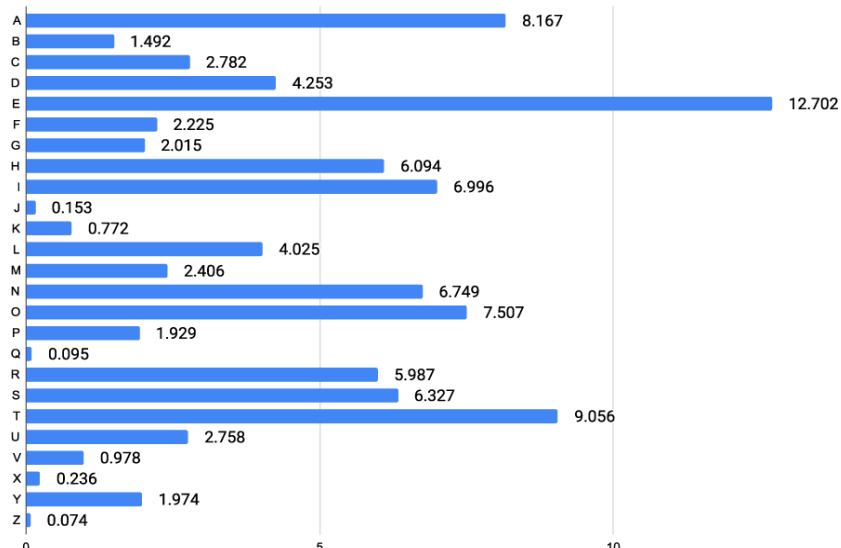
- Single letter: One-letter: **e**
- Diagram: two-letter combination. Most common is **th, an, ed**
- Trigram: Three-letter combination. Most frequent is **the, ing, est**

☞ *Ex: Do decrypt ciphertext*

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXAIZ
VUEPHZHMDZSHZOWSFPAPDTSVPQUZWMXUZHXSXPYEP
PDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ

25

Monoalphabetic Ciphers



Monoalphabetic Ciphers: Cryptanalysis

the frequency data: (single): E,t,a,o,l,s,h,r....

Ex: P:13, Z:11, S:10....

UZQSOVUOHXMOPVGPOZPEVSGZWSZOPFPESXUDBMETSXIAIZ
t a e e t e a t a t e e a
VUEPHZHMDZSHZOWSFPAPPDTSVPQUZWMXUZHXS
e t t a t h a e e e a e t h t a
EPYEPDPDZSZUFPOMBZWPFUPZHMDJUDTMOHMQ
e e e t a t e t h e t

B1: thống kê tần số xuất hiện chữ cái
B2: dựa vào thống kê thì
+ cho chữ cái nào xuất hiện nhiều nhất = E
+ cho chữ cái nào xuất hiện nhiều 2 = T

(E,T là tần suất ở trang trước)

Paintext:

it was disclosed yesterday that several informal but
direct contacts have been made with political
representatives of the viet cong in moscow

27

Mã hóa thay thế: monoalphabetic ciphers

Monoalphabetic Ciphers

Advantages of Monoalphabetic Cipher

- Better Security than Caesar Cipher.
- Provides Encryption and Decryption to data.
- Monoalphabetic Cipher maintains a frequency of letters.

Disadvantages of Monoalphabetic Cipher

- Monoalphabetic ciphers are easy to break because they reflect the frequency data of the original alphabet.
- Prone to guessing attack using the English letters frequency of occurrence of letters.
- The English Language is used so the nature of plain text is known.
- Less secure than a polyalphabetic cipher.

28

Playfair Cipher

- 🗨️ Invented by British scientist Sir Charles Wheatstone in **1854** (name of his friend - Baron Playfair)
- 🔗 Best-known *multiple*-letter encryption cipher
- 🔗 Treats digrams in the plaintext as single units and translates these units into ciphertext digrams
 - Ex: lo ve => dg tu
- 🔗 Based on the use of a 5 x 5 matrix of letters constructed using a keyword
- 🔗 Used as the standard field system by the British Army in World War I and the U.S. Army and other Allied forces during World War II

22/08/2024

29

Playfair Cipher: process

🗨️ Ex, using the keyword MONARCHY. Ex: Hellos => he lx lo sx=> cf su pm.
On => na. ar=rm. Oh => hf

M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

I/J nằm cùng 1 ô
MH/Giải mã chung 1 bảng
Chèn 'x' vào khi tách 2 kí tự giống nhau or là kí tự bị lẻ

🔗 Process:

- Fill in letters of keyword *from left to right* and *from top to bottom*, step another letter if a *letter repeated*
- Fill in the remainder of the matrix with the remaining letters in alphabetic order
- Note: I & J: same cell

Khác dòng khác cột thì thay = kí tự cùng dòng vs nó, cùng cột với kí tự kia
Cùng dòng thì mã hóa = cách dịch các kí tự trong bảng xuống 1 lần/ 1 kí tự
Cùng hàng thì mã hóa = cách dịch các kí tự trong bảng qua phải 1 lần / 1 kí tự

22/08/2024

30

Gặp 2 kí tự giống nhau (Cùng dòng cùng cột): thì thực hiện 2 actions: qua trái, lên trên

Plaintext:

- Hello => he l~~x~~ lo
- Bye => by e~~x~~
- i am a teacher => ia ma te ac he rx

Cyphertext

- Hello => he ll ox

22/08/2024

31

Playfair Cipher: Encrypting

Plaintext is encrypted *two letters* at a time, the following rules:

- If a pair is a repeated letter, insert filler like 'X'
ex: balloon -> ba lx lo on
- If both letters fall in the same row, replace each with letter to right (wrapping back to start from end)
- If both letters fall in the same column, replace each with the letter below it (wrapping to top from bottom)
- Otherwise each letter is replaced by the letter in the same row and in the column of the other letter of the pair
- Ex (word)

22/08/2024

32

Playfair Cipher: ex

- Message = Move forward
- Plaintext = mo ve fo rw ar d~~x~~
- message is padded and segmented

x is just a filler

Cipher	Positions	Ciphertext
mo	same rows	mo → ON
ve	diffent rows and columns	ve → UF
fo	same column	fo → PH
rw	diffent rows and columns	rw → NZ
ar	same row	ar → RM
dx	diffent rows and columns	dx → BZ

- Ciphertext = ON UF PH NZ RM BZ

22/08/2024

33

PlayFair cipher: Decrypting

- ∞ According to 2 letters positions in the grid :
- the same line, replace them by the ones on their left (loop to the right if the edge of the grid is reached),
 - the same column, replace them by the ones just above (loop to the bottom if the top of the grid is reached),
 - similar (same column, same line), replace it by ones on their **left and above**.
 - else, replace the letters by the ones forming a rectangle with the original pair. Beginning with the letter on the same line as the first letter to crypt. $L^1L^2 \Rightarrow L1=(rowL^1,colL^2); L2=(rowL^2,colL^1);$

22/08/2024

34

PlayFair cipher, ex

Ex1: EC -> HA, BC -> AB, RU -> GR, **XX->RR**

*	*	*	*	*
*	A	B	C	D
*	E	G	H	P
*	*	R	S	*
*	T	U	X	Z

22/08/2024

35

PlayFair cipher, ex

Decrypt:

- C= Fuvvnxsmunvtamxasuott, K=security
- C= Fwvvnnonmicvkwnnzkrpruu, K=network
- C= Faxxeofwomorecmctmqevv, K=computer
- C= Kgwwnydpbradbfrsckpmzz, K= Information
- C= Kbvvpportewtdzepzdempcc, K=password

22/08/2024

36

Playfair Cipher: Security

- ✎ Security *much improved* over monoalphabetic
- ✎ Since have $26 \times 26 = 676$ digrams
- ✎ Would need a 676 entry frequency table to analyze (versus 26 for a monoalphabetic)
- ✎ Correspondingly more ciphertext was widely used for many years eg. by US & British military in WW1
- ✎ It can be broken, given a few hundred letters
- ✎ Since still has much of plaintext structure

22/08/2024

37

dạng đa bản

Vigenère Cipher: polyalphabetic

- ✎ Best known and one of the simplest **polyalphabetic** substitution ciphers
- ✎ In this scheme the set of related monoalphabetic substitution rules consists of the 26 Caesar ciphers with shifts of 0 through 25
- ✎ Each cipher is denoted by a *key letter* which is the ciphertext letter that substitutes for the plaintext letter

22/08/2024

38

Bảng này có định cho mã hóa và giải mã

Vigenère Cipher Table

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

22/08/2024

39

Vigenère Cipher: Example

- To encrypt a message, a key is needed that is as long as the message
- Usually, the key is a *repeating keyword*
For example,
 - the keyword: *deceptive*, **Độ dài key phải = độ dài plaintext**
 - the plaintext: *we are discovered save yourself*
- key: *deceptivedeceptivedeceptive*
- plaintext: *wearediscoveredsaveyourself*
- ciphertext: *Z I C V T W Q N G R Z G V T W A V Z H C Q Y G L M G J*
- It works as follows: (look into Vigenère table)
 - Row d + column w -> Z
 - Row e + column e -> I

22/08/2024

40

Vigenère Cipher: Decrypto

- ✎ One locates the first letter of the key in the left column, and locates on the row the first letter of the ciphered message. Then go up in the column to read the first letter, it is the corresponding plain letter.
- ✎ One continues with the next letters of the message and the next letters of the key, when arrived at the end of the key, go back to the first key of the key.

22/08/2024

41

Vigenère Cipher: ex

- ✎ Ex: K= KEY. C= NGMNI.
 - Locates the letter K on the first column, and on the row of it, find the cell of the letter N, the name of its column is D, it is the first letter of the plain message.
 - continues
 - The original plain text is DCODE.

22/08/2024

42

Kĩ thuật dịch chuyển

Transposition technique



Nguyen Thi Thanh Van - Khoa CNTT

22/08/2024

Rail fence

🔗 **Rail fence** technique: the simplest such cipher

- the plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.

- For example, to encipher the message

Khóa là 1 số

meet me after the toga party

with a rail fence of **depth 2**, $k=2$ $k=2$ là viết chuỗi này thành 2 dòng, viết theo kiểu zig zag

- we write the following:
m e m a t r h t g p r y
e t e f e t e o a a t

- The encrypted message is: MEMATRHTGPRYETEFETEOAAT

🔗 Decrypted ?

dòng đầu

dòng 2

22/08/2024

44

Transposition technique

∞ A more complex scheme:

Chia (k chạy từ 1 đến length) để tìm giá trị của k

- write the message in a rectangle,
- row by row, and read the message off,
- column by column, but permute the order of the columns.
- The **order of the columns** then becomes the **key** to the algorithm.

∞ For example,

Key:

Plaintext:

4	3	1	2	5	6	7
a	t	t	a	c	k	p
o	s	t	p	o	n	e
d	u	n	t	i	l	t
w	o	a	m	x	y	z

∞ Cipher text: TTNAAPTMTSUOAODWCOIXKNLYPETZ

22/08/2024

45

Lấy $\text{length}(\text{cipher text}) / \text{length}(\text{key}) \Rightarrow$ tìm ra số dòng

Taxonomy of Cryptography

The type of operations used for transforming plaintext to ciphertext

Substitution

Transposition

The number of keys used

Symmetric, single-key, secret-key, conventional encryption

Asymmetric, two-key, or public-key encryption

The way in which the plaintext is processed

Block cipher

Stream cipher

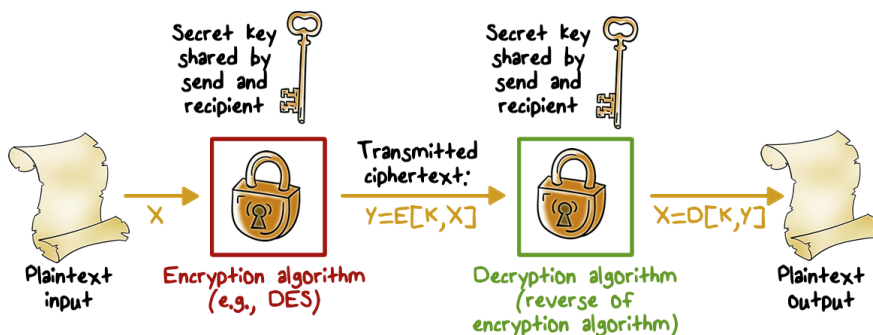
Symmetric & Asymmetric Encryption

- ↻ **Secret key cryptography: one key** same key for encryption and decryption
- ↻ **Public key cryptography (Asymmetric) : two keys**
 - **Public - key**, **Key public dùng cho mã hóa, xác minh**
 - everyone can know and
 - use to **encrypt the message** or
 - to **check the signature** of key's owner.
 - **Private – key**: **Key private dùng cho giải mã, chữ ký (để xác minh người gửi rõ ràng, ko bị fake)**
 - only owner knows and
 - use to **decrypt the message** or
 - to **create the signature**
- ↻ Public for encryption, private for decryption
- ↻ Private for signing and public for verification

22/08/2024

47

Symmetric Encryption



Comparison of Encryption Algorithms

	DES	Triple DES	AES
Plaintext block size (bits)	64	64	128
Ciphertext block size (bits)	64	64	128
Key size (bits)	56	112 or 168	128, 192, or 256

DES = Data Encryption Standard

AES = Advanced Encryption Standard

A block cipher:

- processes the plaintext input in fixed-size blocks
- produces a block of ciphertext of equal size for each plaintext block.

Comparison of Encryption Algorithms

Key size (bits)	Cipher	Number of Alternative Keys	Time Required at 10^9 descriptions/s	Time Required at 10^{17} descriptions/s
56	DES	$2^{56} \approx 7.2 \times 10^{16}$	2^{55} ns = 1.125 years	1 hour
128	AES	$2^{128} \approx 3.4 \times 10^{38}$	2^{127} ns = 5.3×10^{21} years	5.3×10^{17} years
168	Triple DES	$2^{168} \approx 3.7 \times 10^{50}$	2^{167} ns = 5.3×10^{33} years	5.8×10^{29} years
192	AES	$2^{192} \approx 6.3 \times 10^{57}$	2^{191} ns = 5.3×10^{40} years	9.8×10^{36} years
256	AES	$2^{256} \approx 1.2 \times 10^{77}$	2^{255} ns = 5.3×10^{60} years	1.8×10^{56} years

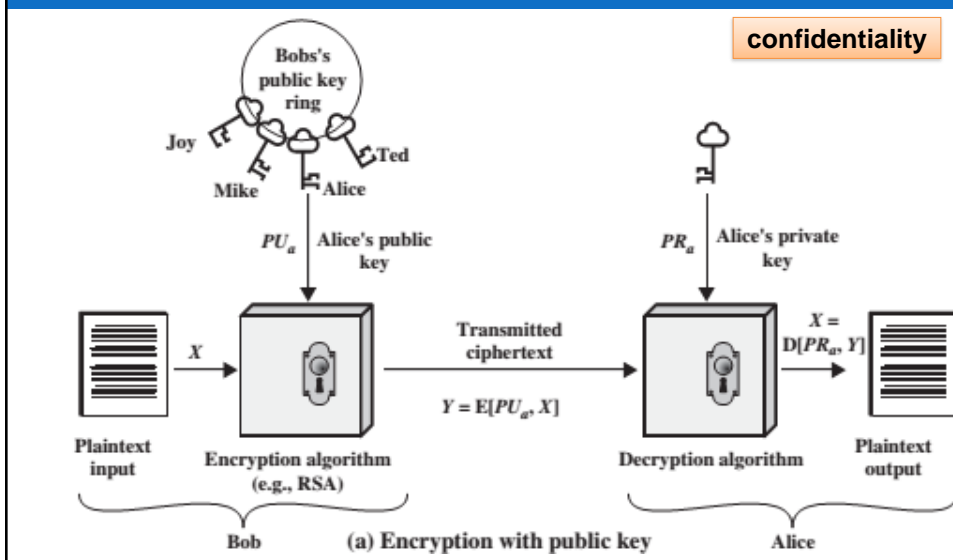


Symmetric Encryption Quiz

Select the correct definition for **each type of attack**:

- | | |
|--|---|
| A. A method to determine the encryption function by analyzing known phrases and their encryption | <input type="checkbox"/> known-Plaintext attacks |
| B. Analyzing the effect of changes in input on the encrypted output | <input type="checkbox"/> chosen-Plaintext attacks |
| C. Compare the ciphertexts with its known plaintext | <input type="checkbox"/> differential cryptanalysis |
| D. A method where a specific known plaintext is compared to its ciphertext | <input type="checkbox"/> linear cryptanalysis |

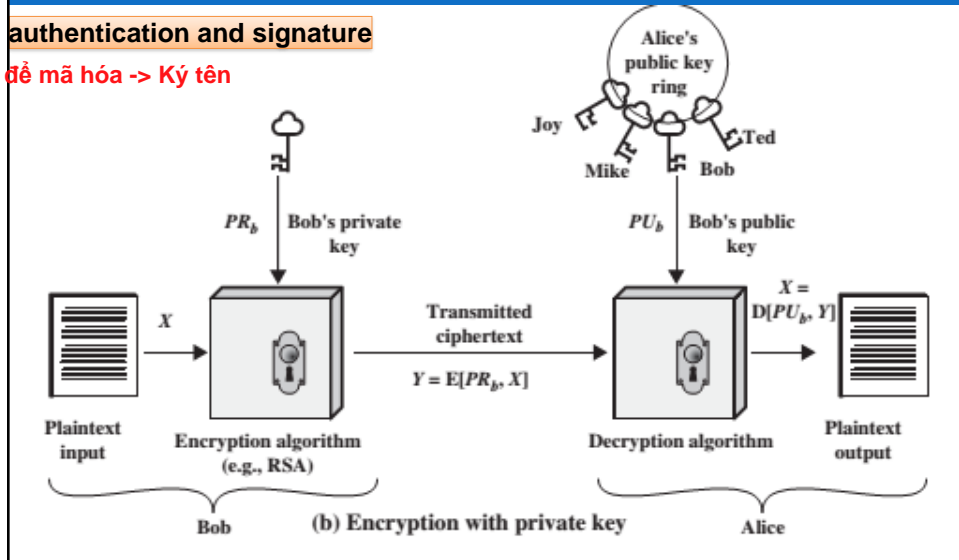
Asymmetric Encryption with public key



Asymmetric Encryption with private key

authentication and signature

Dùng private key để mã hóa -> Ký tên



What is Hash Functions

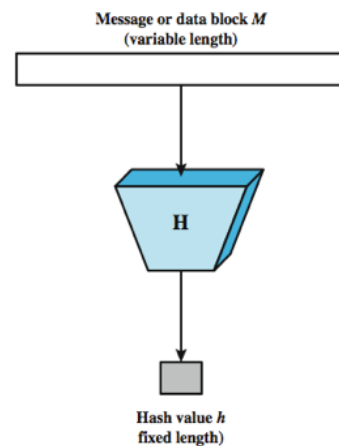
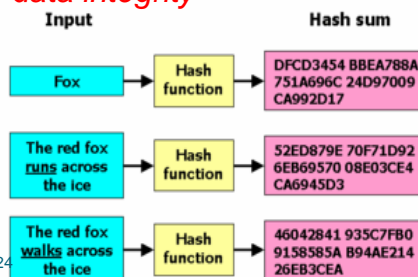
Cách giải là thử all, thử sai thì quay lại thử tiếp

- A hash function maps a *variable-length* message into a *fixed-length* hash value, or message digest

$$h = H(M)$$

- The *principal* object:

- data integrity*



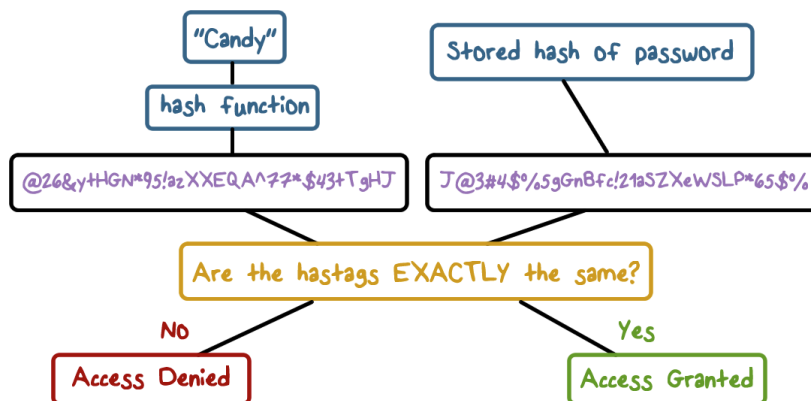
22/08/2024

54

Hash Functions

- hash functions and several common hash functions used in modern digital signature algorithms
- Compute message digest of **data of any size**
- **Fixed length output**: 128-512 bits
- Easy to compute $H(m)$
- Given $H(m)$, no easy way to find m
 - **One-way function**
- Given m_1 , it is computationally infeasible to find $m_2 \neq m_1$ s.t. $H(m_2) = H(m_1)$
 - **Weak collision resistant**
- Computationally infeasible to find $m_1 \neq m_2$ s.t. $H(m_1) = H(m_2)$
 - **Strong collision resistant**

Hash Functions for Passwords





Hash Function Quiz

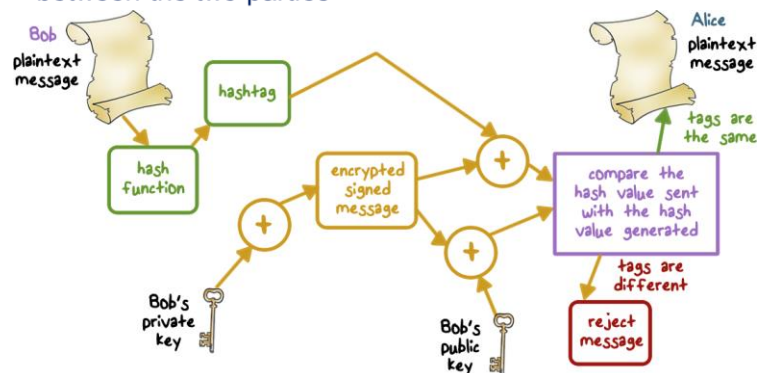
Which of the following characteristics would **improve password security**?

- ☐ Use a one-way hash function
- ☐ Should not use the flood effect
- ☐ Should only check to see that the hash function output is the same as stored output

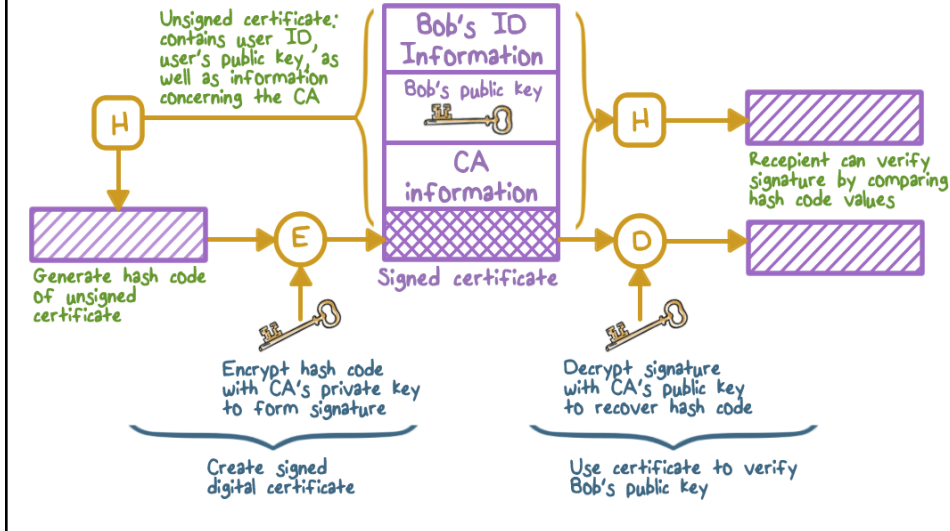
Digital Signatures

cryptosystems implement digital signatures to provide:

- o proof that a message originated from a particular user of the cryptosystem
- o to ensure that the message was not modified while in transit between the two parties



Digital Signatures



Summary

- History of Encryption
- Substitution Techniques: Caesar Cipher, Monoalphabetic Ciphers, Playfair Cipher, Polyalphabetic Ciphers
- Transposition Techniques: Rail Fence
- Symmetric and asymmetric encryption
- Hash
- Digital signatures

Các chương đầu thì tập trung 3 mục đầu này

Học ở chương gần cuối (3 chương cuối cùng)

Chuẩn bị cho chương 3: software security - tập trung vào tìm hiểu sự an toàn khi viết phần mềm C, cài 1 máy ảo ubuntu, tải trình biên dịch gcc (thật ra có bản ubuntu đã có cài sẵn gcc, nếu chưa có thì tự cài đề làm lab)

22/08/2024

60